Method of security processing of data flow such as e.g. MP3 data stream by transmitting processes data stream back to external device that recombines of processes part with major fraction to produce flux of output information

Publication number: FR2812147
Publication date: 2002-01-25

Inventor: GRIEU FRANCOIS; MOLY JACQUES
Applicant: INNOVATRON SA (FR)

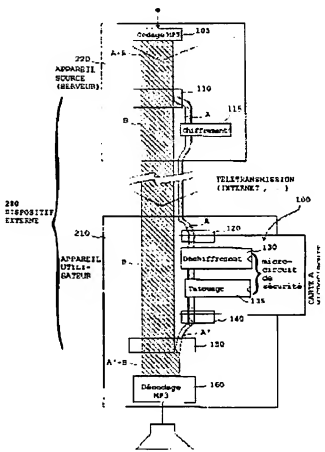
Classification:
- **international:** ***H04N7/16; H04N7/167;*** **H04N7/16; H04N7/167;** (IPC1-7): H04L9/16; G06K19/07; H04N1/44; H04N7/16
- **European:** H04N7/16E2; H04N7/167D

Application number: FR20000009479 20000719
Priority number(s): FR20000009479 20000719

Report a data error here

Abstract of **FR2812147**

A small fraction of a transmission (120) is sent to a microchip, which decodes and watermarks (130,135) the small fraction. The processed part is transmitted (140) to an external device that recombines (150) of the processes part (A') with the major fraction (B) in order to produce a flux of an output information (A'+B) for MP3 decoding (160).



Europaisches Patentamt
European Patent Office
Office Européen de Brevets

Description of FR2812147	Print	Copy	Contact Us	Close

Result Page

The invention relates to a process of treatment of a naked flow of information

meric by a safety circuit.

It relates to particularly the treatment of information représentati-

ves of reproducible sequences such as secuences audio, video, tex-

tuelles or similar. One will describe the invention mainly within the framework of audio sequences

because it is the most immediate application taking into account the capaci-

t-pieces current of the networks of diffusion; however, I' invention can be

transposed directly to acquisition of other types of sequences, No

tamment of video data (fixed images or animated images of télévi-

Sion) or of textual sequences. It applies ir the same way to ac

quisition of sequences forming data files of nature informati-

that, for example of the data necessary to the remote loading of a logi-

sky, or to allow the execution by the user of a software requiring a data exchange with a distant site; this application lends itself

in particular with the field of the downloaced electronic plays.

It frequently happens that one wishes to carry out one or more draft

ments on such a flow of information, treatment (S) operated (S) in a microphone

safety circuit, for example the microcircuit of a smart card, able to store information in a permanent memory and to carry out cryptographic calculations on the information (key) stored in

this microcircuit, and nonreadable of the outside of the microcircuit.

The treatments which one wishes to carry out are in particular: - deciphering and/or rechiffrement of flow; - the control or the generation of a certificate or electronic signature of flow;

- ?tattooing?, namely the encoding or decoding of information auxi-

liaire in fillgree of flow (i.e. superimposing on flow one informed

▲ top

tion unperceivable with the human directions, but which one can detect by suitable means); such systems for example are described in the USA-5 687.191 (Solana Technology Development Corp.);

- I' extraction or addition of information to flow by demultiplexing or multi-

plexage;

- all operations usually carried out in a microcircuit of

curity, in particular controls of any nature, accounting, pay

lles, storage.

The interest to carry out these operations in a microcircuit of safety is in general to hide part of the information used in the treatment,

and/or to guarantee that such or such treatment is well carried out according to D's

gles imposed. Thus, in an example of application which one will explain more in detail thereafter, one wish that a flow of music, digitized and compressed according to

ISO/IEC 11172-3, is quantified, transmitted to identical to several destinatai-

LMBO, deciphered and tattooed by information of identification from the microphone

circuit entrusted to each user. The interest to carry out the operations of deciphering and tattooing in a microcircuit of safety, rather than in a microcomputer for example, is that one is thus ensured that the flow of information deciphered

and not tattooed is not accessible, not mere

of course that the key of deciphering, nor that being used for encoder tattooed it

Ge. The need for such treatments brings out in particular from the WO-A-00/11866 for ?protected Device decoder of quantified and compressed information?

(Innovatron SA), which describes an implementation particularly avan-

tageuse of the deciphering and the decompression of the signals to the means

of a chart with microcircuit.

One can also consider the problem consisting in extracting from an audio or video flow of information relating to the management of rights of exploitation, such as identification of the authorized receiving device, a number of copies

authorized, price, and to carry out operations such as controls iden-

tification and/or of the rights of copy, decrementation of the number of copies

authorized, payment, tattooing of the remaining number of copies and/or I

dentifiant receiving device authorized for resulting information. The need for such treatments is apparent in the US-A-5 892.900 (Intertrust

Corp technologies.).

A realization according to standard techniques' would consist in transferring

I' information with the microcircuit, there to carry out the treatments and to restore the infor-

treated mation. It encounters two practical limitations:

- speed transmission of the existing readers of microcircuit: those

Ci usually communicate with a flow of 9,6 kbit/s, and the productive flow is even lower, about 5 kbit/s, whereas, in an example of compressed music with 128 kbit/s, one would need a flow much higher, of 256 kbit/s (factor 2 coming from the double entering flow

and outgoing), to process the data at the speed of listening.

- processing capacity (deciphering and tattooing) of the microcircuit

is limited.

One of the goals of the invention is to mitigate this difficulty of practical implementation, by a means making it possible to reduce the quantity of information

exchanged with the microcircuit without to compromise the carac-

tère sedentary of the treatments carried out in the microcircuit - notam-

ilies without increasing the risk of fraud.

Primarily, I' invention proposes to select a small fraction of the information (typically less than 20% and for example between 5% and 1%, even less than 1%) which will be extracted from total flow for transmission and treatment by the microcircuit, then to recombine it with the untreated part of flow. Fraction of flow extracted for treatment in the chart

will be selected so that its presence is important, even essen-

tielle, for the good realization of the desired functions of exploitation of

the whole of information. For example, in the case of a flow of musi-

that digitized, in the absence of a correct sedentary treatment by the bus

you, of the passages of the music would miss periodically, or

stripe periodically deformed, returning the reproduction of the music

unacceptable.

In this manner, it is possible to carry out relatively complex treatments (deciphering, tattooing, calculation of key, etc) with charts with microcircuit and readers traditional, whose processing capacity would be largely insufficient to allow a treatment of the unit

flow, which makes possible the implementation of these treatments which

stripe differently excluded.

More precisely, I' invention aims at a process of treatment of a flow of in

formations by a microcircuit of safety, in particular a microcircuit of this microcircuit, smart card cooperating with an external device ready to produce the flow of information in the form of numerical data and with

to use this flow of information after treatment by the microcircuit, caracté-

small channel by the following stages: a) by the external device, production of the flow of information, b) by the external device, separation of the incidental flow of information in

two distinct fractions, with a minor fraction and a fraction my

jeure, major fraction having a size and/or a flow of infor-

mation notably higher than the minor fraction,

c) transmission of the minor fraction of the external device to the microcir-

cooked, D) within the microcircuit, sedentary treatment of the minor fraction, E) transmission of the minor fraction treated of the microcircuit with the external device, F) by the external device, recombination of the minor fraction treated with the major fraction so as to produce a leaving flow of information,

g) by the external device, use of the leaving flow of information.

According to various advantageous implementations subsidiary:

- the sedentary treatment of the stage D) is a treatment of the group COM

taking: deciphering or coding of flow; control or generation

of a certificate or electronic signature of flow; encoding or decoded

Ge of auxiliary information tattooed in flow; extraction or addition of information to flow by demultiplexing or multiplexing; validity check of flow; management of rights of exploitation of information of flow; combination of two or several of the preceding treatments;

- the external device comprises an apparatus source and an apparatus utili-

sator distinct, the microcircuit cooperating with the apparatus user, the stages has) and b) are implemented in the apparatus source, and the stage F) is implemented in the apparatus user; - after the stage b) of separation and before the stage c) of transmission, it is

envisaged a stage of treatment, in particular of coding, frac-

tion minor (A) by the external device, the stage D) of sécu- treatment

ritaire implemented within the microcircuit being a stage of a symmetrical treatment, in particular a stage of deciphering; - the sedentary treatment of the stage D) includes a transcribing of key,

comprising a deciphering with a first key then a rechiffre-

lies with one second key;

- the separation of the stage b) comprises a temporal separation, aperture

rée by incidental flow division in intervals of time, and/or a separation function of the informational contents of the data component

incidental flow, operated by retrieval of fields of data of Na

predetermined ture; - the separation of the stage b) and/or the sedentary treatment are a function

parameters influencing the perceptibility of separation and/or the trai-

tement and selected in order to reduce perceptibility of it;

- the sedentary treatment of the stage D) also includes/understands the produc-

tion of a key ready to allow the deciphering of the major fraction by the external device;

- the size and/or the flow of information of the minor fraction are infé-

laughers at 20% of the total flow, preferably ranging between 5% and 1% of

total flow, advantageously lower than 1% of total flow.

One now will describe an example of implementation of the invention, in

reference to the annexed drawings.

Figure 1 illustrates in a diagrammatic way the various stages of the procé-

dé of the invention.

Figure 2 illustrates, in the form of building blocks, various elements

implied in implementation a particular of the process of the invention.

The setting in œuvre of the invention implies, like illustrated figure 1, at least two distinct bodies, namely a microcircuit of safety 100 and,

in addition, a unit which one will call ?external device? 200, horn

respondant with the external, nonprotected environment or partially

curized, of this microcircuit 100.

The microcircuit of safety can be for example a ST16SF48 of STMi-

croelectronics, inserted in a chart according to ISO/IEC 7816-1 to -3 and connected to its environment by a card reader to microcircuit conforms to

these standards or in an equivalent way (as well removable as per-

manente), for example through a bus of the type USB.

In the example which one will describe, the external device 200 consists of a ?apparatus user? 210 and of a ?apparatus source? 220 connected to each other by a transportation route such as a connection Internet or all

another way of télétransmission.

This implementation in which the external device 200 is made up

of two distinct and distant bodies 210 and 220 is however not li

mitative, and the invention applies as well to the treatment of information

produced and used by a single apparatus.

In the example which one will describe, I' apparatus user 210 can notam-

lies being a device of the type ?tuner Internet? as described in the WO-

A-00/11867 for ?Process of delivery certified of an audio, video or textual sequence? (Innovatron SA) and WO-A-00/11868 for ?Process of

delivery and of payment of an audio, video or textual sequence " (In

novatron SA). These requests describe means making it possible to acquire for listening of the audio sequences, typically of musical works

such as pieces of music or individual beaches of one in

registrement, suitably selected by the use:. Pieces

of music are downloaded in the form of packages of data numéri-

ques possibly signed, quantified and compressed, and transmitted since

a central site (apparatus source) with the apparatus user.

The apparatus user 210 comprises means, integrated to this end or

separated, of sound reproduction, various circuits of decompression, die

encoding, payment, access control, etc, in particular of the circuits implementing one or more charts at microcircuit, as well as means of connection to a distant site (central site or delocalized in several sites). The remote loading is typically carried out via Internet, i.e.

by the inter-connected world networks connecting sites ard used

teurs by variable and multiple routings for the transmission of gift

born in numerical form.

The apparatus source 220 is for an example a configured microcomputer

out of waiter Internet, or even a simple storage medium such as C

dérom or DVD-ROM.

Original information intended to be treated first of all is digitized and advantageously compressed and coded, for example, in the case of

music, by a coding ISO/IEC 11172-3 to bush-hammer 3 (?MP3?) (stage 105).

In a way characteristic of the invention, flow resulting 110 is then separate in two distinct fractions, a minor fraction A (representative for example between 5% and 1% in volume of total flow), and a major fraction B (representative thus respectively between 95% and 99% of total flow A+B). Flow A is defined so as to contain information

necessary, even essential, with a correct exploitation of flow glo-

ball A+B. The separation of stage 110 can be operated various manners,

who can with the surpluses being combined between them.

In a first alternative, separation is a temporal separation.

Information is then divided into intervals of time corresponding to

time of transmission or, for an audio or video flow, with the time of LMBO

titution with the human directions. A predetermined fraction of these intervals constitutes A, and the remainder B. This temporal selection finds its justification in the fact that an audio or video message periodically cut down by a significant part of its contents becomes unusable. For example, it

flow A retains intervals of 0,2 second every 4 seconds.

As the flow of audio or video information is frequently, by its Co

dage even, structured screens representing of the intervals of distinct times (called ?frames? in ISO/IEC 11172-3), this temporal cutting then reverts retaining for flow A a fraction of the screens: for example, if a screen lasts 0,025 S, then flow A will retain 8 screens on

160. This is an example of a case O it can be advantageous that the frac-

tion minor represents between 5% and 1% of total flow A+B, this fraction being sufficiently important to ensure an unacceptable degradation of the contents if it is not reproduced, while strongly reducing

charge of the microcircuit.

In one second alternative, separation is a separation by nature of information.

The flow of information is divided by a factor 200, which allows D

duire the load of the microcircuit to less than 1% of total flow A + B while guaranteeing safety, by preferentially selecting for flow A information of predetermined nature which are most important for the intelligibility of flow by the human directions and/or those adapted to

treatment considered and/or those necessary for the exploitation of in

seem information and/or whose reconstitution in the event of deterioration is most difficult. For example, according to ISO/IEC 11172-3 each screen is cut out in many fields, and to make completely unusable

an audio flow ISO/IEC 11172-3 to bush-hammer III it is enough to quantify the Huf- fields

fmancodebits (see 2.4.1.7 of the standard, page 19), or the only bits signx and signy, or a predetermined number of selected bits signx and signy as being those of certain values of the index/, for example iike a predetermined number of those for which Ixl and

IYI are largest, possibly while being restricted with one inter

valle of/.

In the case of a consistent treatment in a tattooing, one will retain in

flow A data the sizes which, taking into account the sys-

tème, is to be modified for the inscription of the filigree it will act for example of information in a predetermined frequency band and/or that whose amplitude is largest and/or most constant and/or in

iimit of a celling of quantity or flow of information predetermined Li

mitant the quantity of information included in flow A.

Moreover, the two alternatives which one has just described can be combi-

born between them, in various ways. As follows:

- one can simply retain only one fraction of information (?

lection by nature " above) of a temporal fraction (?temporal selection? above) of flow, which multiple effects of reduction of flow A. - one can also carry out a temporal selection according to the adequacy with the treatment to be carried out: the intervals of time of flow are examined

to determine their adequacy with the treatment to carry out (such as your

warping) and one preferentially select those of the intervals of the flow which is ready to undergo the treatment (with a minimal degradation of perceived quality and/or a better capacity of coding, these parameters varying considerably according to intervals' of time), within the limit of a predetermined ceiling limiting the quantity of information included in flow A. The combination of the two techniques of selection can make it possible to have for A a fraction even weaker than 1% of total information, it

who allows the use of microcircuits and readers of microcircuit ac

tuellement available, without awaiting future progress of their perfor-

mances, while maintaining the level of safety necessary for the treatment

(deciphering and tattooing).

Before transmission with the apparatus user, it is often useful to envisage, on the level of the waiter, an additional stage 115 of treatment of flow A, for example a stage of coding by means of a secret key K and of a symmetrical algorithm.

The flows A and B thus prepared by the waiter source 220 are then trans

put at the apparatus user 210, which thus receives jointly these two flows A and B, for example multiplexed to allow their transmission on

a common channel.

With reception, flow A is isolated and transmitted (into 120) to the microcircuit from

curity 100. This one deciphers then flow A (stage 130) by means of the key K which it contains or which it is able to recompute. If one wishes moreover to tattoo the music before restoring it, the microcircuit operates then one

tattooing (stage 135) by inscription in filigree in flow A of a identi-

trusting clean the microcircuit (or of another identifier specific to the chart and/or the user)

Resulting flow A' is transmitted in return (into 140) to the apparatus user.

This last combines flows A' and B (stage 150) and transforms the whole into a reproducible aural signal, for example by

decoding ISO/IEC

11172-3 to bush-hammer 3 (?MP3?) of stage 160.

The process which one has just described can be the subject of different

adaptations or improvements.

Thus, in the case of a temporal selection, it can be useful to a stage

additional (located after coding 115) to reorder the seg-

ments so as to allow the easiest possible restitution, without waiting at the beginning and with a minimum of memory in the device of restitution. Let us take the example of screens numbered consecutively from 01 to 30, the multiple screens of 10 belonging to flow A. It will be useful to this additional stage to reorder flow in the order:

10 01 02 03 04 05 06 07 08 09 20 11 12 13 14 15 16 17 18 19 30 21 22

23 24 25 26 27 28 29.

This way, the sound restitution of screens N 01 to 09 will be able to be made while screen N 10 will be transmitted and treated by the microcircuit

(stages 120 to 140), relatively long operations.

In the same way screens N 20 and 30 will be treated during the restitution of

screens N 11 to 19 and 20 to 29.

Another improvement consists in combining the technique of the invention

with a different technique, in itself known and used notam-

lies in television with toll, aiming at reducing by another means the quanti-

t-piece of information handled by the microcircuit (but in the only case

of a treatment of conditional deciphering).

In this known technique: - a key K is chosen (possibly variable in time); - one quantifies audio flow or video F with this key K, producing F'; - one quantifies the key K with another key, producing K' - one combines F' flow and the K' key by multiplexing; - one transmits the unit to a decoder; - the decoder separates F' and the K' key; - the decoder transmits the K' key to the microcircuit; - the microcircuit deciphers the K' key, producing K; - the microcircuit transmits the key K to the decoder;

- the decoder deciphers F' flow, producing flow F of origin.

It will be noted that in this known technique useful information F (audio or video) does not forward in the microcircuit, whereas it does it partly

in the system object of this invention (with the advantage caracté-

ristic to allow in the microcircuit even an arbitrary treatment,

such as a tattooing, useful information).

Thus, the information restored in this known technique is identical to the information of origin, whereas the invention allows its partial treatment in the microcircuit. In practice, the combination of information resulting from the microcircuit and principal flow is done by deciphering in the technique of television with toll, whereas it is done by addition or multiplexing

in a form of the invention.

One can usefully combine this technique known with that of pre

invention feels, to decipher flow B in particular. One can by exem-

ple to add to the preceding system the following stages: - with the waiter source, upstream of stage 115 of coding: - one chooses a random key KB, - one quantifies flow B with KB, and - one multiplexes the value of KB with A; - at stage 115, one quantifies KB and A together with K (one could envisage a separate stage); - one transmits KB' and A quantified to the apparatus user (one could envisage a separate stage); - at stage 120, one transmits KB' and A quantified together to the microcircuit of safety (one could envisage a separate stage);

- at stage 130, one deciphers KB and A (one could envisage a stage

avoided); - at stage 140, one transmits KB and A' to the apparatus user (one could envisage a separate stage); - upstream of stage 150 of recombination: - one extracts key KB from A' flow, in a symmetrical way to that of the multiplexing by the waiter source; and - one deciphers flow B with KB, in a symmetrical way to that of

coding by the waiter source.

It will be noticed that, if one combines the coding of flow B and the techni-

that of regrouping of the screens exposed higher, key KB chif-

frant screens N 11 to 19 must be in block N 10, and not in

block N 20.

It can be useful to provide that the microcircuit deciphers the K' key, giving

K, and the rechiffre in a different way, giving K ".

In addition, in supplement of the keys of coding, from information related to flow (such as reproduction rights) can be extracted from

flow and treated by the microcircuit.

Thus, treatment 30 can include/understand: - deciphering with a first key, and

- rechiffrement with a second key.

This transcribing of key authorizes for example the deciphering in the device user of a flow coming from the waiter, in particular afterwards

payment, rechiffrement limiting its later re-use to another ap-

similar specifically indicated by the key of recharging (for example

a particular walkman).

Figure 2 illustrates, in the form of building blocks, various elements implied in implementation a particular of the process which one comes

to describe.

This configuration is intended to allow the diffusion of contents mul-

timédia (audio, video, plays, etc) of the apparatus source (waiter) 220. O these contents multi-media is prepared and made available in the manner that one will describe, towards the apparatus recipient 210 of a customer: - by making sure that the contents will be available only for the customers who will have discharged a right of visualization, - while also allowing to guarantee the payments and to make comply with the rules defined by the beneficiaries (for example a limited number of authorized visualizations),

- by getting a certain traceability finally allowing, in the event of frau-

of, to be able to go up with the waiter and/or to determine the purchaser with the ori-

gine of the copy.

The apparatus recipient 210 of the customer is a material unit and software made up around equipment of the type known such as microcomputer, numerical decoder of TV (in particular of the type ?set signal box?), or

telephone portable ready to exchange numerical data formed

lies to standards GSM, WAP, GPRS, UMTS or others.

With this equipment are associated: - an application software customer 211, microcircuit 100, - possibly a means of storage of mass 213 such as hard disk, memory flash, etc, - a peripheral 214 of restitution of the multi-media contents, for example

monitor of television, audio amplifier, numerical assistant per-

* sonnel, engraver of compact disk, etc The multi-media contents are first of all prepared on the level of the waiter

source 220 in the following way.

These contents, indicated ?contained value? on figure 2, are accompanied by ?rules of use? which define the restrictions of use, the number of copies used, the duration of time limitation, etc These rules can be possibly nonspecific rules, applied by defect when the contents of value are associated no clean rule.

The multi-media contents can also include/understand information, die

signed ?contained without value?, not recuiring measurements of protec-

tion particular, for example biography of the interpreter, words of a song, jacket of presentation, etc The rules of use are incorporated in the contents of value, for example and

in a way in itself known by tattooing, then the unit is die

half-compartment in blocks, signed and quantified, to produce finally: - on the one hand contents of value, in the form of signed and quantified blocks, these contents of value incorporating the rules of use,

- in addition, a ?title of associated access?, which will make it possible to control ac

these with the multi-media contents and its restitution by the apparatus recipient

in the manner that one will indicate low (the term ?titrates? being enten-

in its legal meaning (as in ?transport document? or

?evidence of indebtedness?), i.e. like certificate noting an act ju-

ridic or material likely to produce effects - here authorized it

tion of reproduction or duplication of the contents), - and possibly the contents without value, simply cut out in

blocks.

This whole of data is stored by waiter 220.

The transaction waiter-customer is carried out in a way protected between the ser-

vor and microcircuit 100 according to techniques' in themselves known, the application software customer 211 being used as footbridge enters the waiter and

the microcircuit.

To ensure the security, the microcircuit and the waiter exchange certificates, with for example: - a first certificate, microcircuit towards the waiter, to certify that the user of the microcircuit discharged the price well corresponding to the precisely identified contents of value, and - a second certificate, waiter towards the microcircuit, to transmit to this last the title of access, this title possibly which can contain one

key of decoding.

These certificates are signed and encrypted using keys preserved of one

manner protected in the microcircuit and the waiter. Transac-

tions between these two bodies are thus made safe, even through one

nonsure channel (telephone network, cabled network, Internet, etc).

Once these operations carried out, I' together of the blocks of the contents of

mandé (contained value and contents without value) is transmitted to the appa-

reil recipient.

Any operation in source or bound for a peripheral, y COM

taken the local peripheral of restitution 2:.4, can be done only with through

microcircuit 100, this last answering to this end only COM

mandes duly signed and authenticated.

After preparation and transfer of the multi-media contents, I' apparatus destinatai-

Re has the contents of value, encrypted with the rules which must in D

to gir the access, and possibly of a whole of nonsecret information

(contents without value, which can be posted by the peripheral of restitu-

tion 214, or simply ignored).

One first of all will describe an implementation in which the contents of value are restored in ?streaming? i.e. restored in a form

understandable with the human directions progressively with its reception, sensi-

blement at the speed to which it is transmitted, without permanent storage

in the device user (which stores only one limited quantity of infor-

subdued, for example correspondent at one second of restitution for

to deaden the fluctuations of short duration of the transmission resource).

The blocks are transmitted to the apparatus recipient which emits an order of deciphering to the microcircuit while placing the block to him. The microcircuit

accept these orders of course only if they were suitable

lies signed and authenticated. It calculates the signature of the block and checks the conditions of access, in particular the fact that the user has the right well to receive the contents in ?streaming? and that it discharged well payment of the rights of reading; it uses for that the title of access which it received following the payment, with the rules which were tattooed and/or included in

contents of value.

In accordance with the present invention, the contents of value incorporating the rules are divided (stage 110 of figure 1) into two distinct flows A and B in a relevant way, i.e. so as to make not exploitable flow

B alone, or flow A+B, without A not being treated later on by the mid- one

crocircuit.

Flow B (major fraction, typically 95 or 99% in volume of total flow A+B) is quantified with a first key, or possibly left in light. On the other hand, the flow A, which must be treated with the maximum of safety,

is quantified (stage 115 of figure 1), just as the rules and the pre one

key mière above mentioned, in order to be decipherable later on only by

the microcircuit of safety.

In a way characteristic of the invention, only flow A is transmitted to mid-

crocircuit, or it will be deciphered and tattooed (stages 130 and 135 of figure 1).

Possibly, the microcircuit also can rechiffrer flow A with

a key associated with the particular peripheral of restitution 214.

In addition, the microcircuit restores and transmits to the apparatus user the first above mentioned key, i.e. that which allows the deciphering of flow

B with the case O this one was not transmitted in light.

This deciphering of flow B is operated outside the microcircuit, whose memory sizes and of treatment would be insufficient to ensure

this operation in real time.

Peripheral 214 can then restore the multi-media contents.

When the ?streaming? possible or is not wished, the contents are simply downloaded, i.e. corresponding information is stored completely and in a permanent way in the means of

storage 213 for later restitution.

The procedure described above is then adapted in the following way.

The application software customer 211 is used as footbridge between the waiter source 220, microcircuit 100 and the peripheral of restitution 214.

peripheral 214 and microcircuit 100 possibly can identi-

proud, for example by exchange of certificates containing of the data risk

toires. They can also exchange keys between them for communi-

quer in a quantified way.

The application software customer 211 transmits signed orders and

encrypted with microcircuit 100 by attaching the blocks to it. Of course, the mid- one

crocircuit accepts these orders only if they were suitably

signed and authenticated.

The microcircuit calculates the signature of the block and checks the ac conditions

these, in particular the fact that the user has the right well to copy the tale

naked and that it discharged well payment of the rights of reading. It uses for that the title of access which it received following the payment, with the rules

who were tattooed or included in the contents of value.

If all the conditions are respected strictly, the microcircuit deciphers flow A, the rechiffre possibly with a key associated with the peripheral with restitution and transmits these contents to the peripheral 213, which can then store these multi-media contents, from which the restitution will be carried out later on. In the case O the user tries to transfer the contents downloaded towards another means from storage, microcircuit 100 will authorize the recopy only for one contents of which it has the rights of access, unless it does not act

of marked contents ?free of rights?. In the case O the rights are pre

sents, it does not have in theory a recopy there, since the contents are already

stored on the means of storage of the apparatus of the user.

Europäisches Patentamt
European Patent Office
Office Européen de Brevets

Claims of FR2812147	Print	Copy	Contact Us	Close

Result Page

CLAIMS

1. A process of treatment of a flow of information by a microcircuit of safety (100), in particular a microcircuit of this microcircuit, smart card cooperating with an external device (200) ready to produce the flow of infor-

subdued in the form of numerical data and to use this flow of informed

tions after treatment by the microcircuit, process characterized by the following stages: a) by the external device, production of the flow of information, b) by the external device, separation (110) of the incidental flow of information (A+B) in two distinct fractions, with a minor fraction (A) and a major fraction (B), the major fraction having a size and/or a flow of information notably higher than the minor fraction,

c) transmission (120) of the minor fraction of the external device to mid-

1 5 crocircuit, D) within the microcircuit, sedentary treatment (130, 135) of the minor fraction, E) transmission (140) of the minor fraction treated (A') of the microcircuit with the external device, F) by the external device, recombination (150) of the minor fraction treated (A') with the major fraction (B) so as to produce a flow of information leaving (A'+B), G) by the external device, use (160) of the leaving flow of information

(A'+B).

2. The process of the claim 1, in which the sedentary treatment of the stage D) is a treatment of the group including/understanding: deciphering or coding of flow; control or generation of a certificate or electronic signature of flow; encoding or decoding of auxiliary information

tattooed in flow; extraction or addition of information to flow by die

multiplexing or multiplexing; validity check of flow; management of rights of exploitation of information of flow; and combination of two or

several of the preceding treatments.

3. The process of the claim 1 or 2, in which: - the external device comprises an apparatus source (220) and an apparatus

user (210) distinct, the microcircuit (100) cooperating with the appa-

reil user (210); - the stages has) and b) are implemented in the apparatus source; and

- I' stage F) is implemented in the apparatus user.

▲ top

4. The process of the one of the claims 1 to 3, in which, after the éta-

EP b) of separation and before the stage c) of transmission, it is envisaged one

stage (115) of treatment, in particular of coding, the mid- fraction

neure (A) by the external device, I' stage D) of sedentary treatment put

in work within the microcircuit being a stage of a symétri- treatment

that, in particular a stage of deciphering (130).

5. The process of claim 4, in which the sedentary treatment of the stage D) includes a transcribing of key, comprising a deciphering

with a first key then one rechiffrement with a second key.

6. The process of the one of the claims 1 to 5, in which separation

stage b) comprises a temporal separation, operated by cutting

incidental flow in intervals of time.

7. The process of the one of the claims 1 to 6, in which separation

stage b) comprises a separation function of the informational contents of the data composing incidental flow, operated by extraction of fields

data of predetermined nature.

8. The process of the one of the claims 1 to 7, in which separation stage b) is an at the same time temporal separation and function of the contents informational of the data composing incidental flow, operated by dle cutting of incidental flow in intervals of time and extraction of fields data of predetermined nature.

9. The process of the one of the claims 1 to 8, in which separation stage b) and/or the sedentary treatment (130, 135) is related to Pa rameters influencing the perceptibility of separation and/or the treatment and selected in order to reduce perceptibility of it.

10. The process of the one of the claims 1 to 9, in which draft lies sedentary of the stage D) also includes/understands the production of a key ready to allow the deciphering of the major fraction (B) by the dispo- sitif external.

11. The process of the one of the claims 1 to 10, in which size and/or the flow of information of the mino· fraction (A) are lower than % of total flow (A+B).

12. The process of the claim 11, in which the size and/or the flow of information of the minor fraction (A) are included/understood between 5% and 1% of total flow (A+B).

13. The process of the claim 11, in which the size and/or the flow of information of the minor fraction (A) are lower than 1% of total flow (A+B).

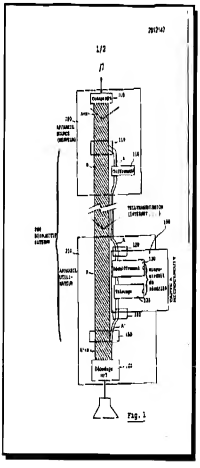


Fig. 1

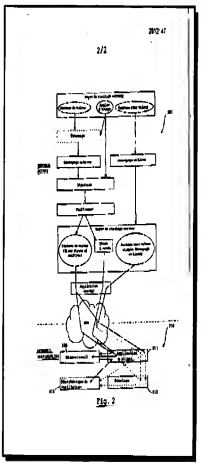


Fig. 2